

(19) 世界知的所有権機関  
国際事務局(43) 国際公開日  
2003年10月9日 (09.10.2003)

PCT

(10) 国際公開番号  
WO 03/083678 A1

(51) 国際特許分類<sup>7</sup>: G06F 13/14, 12/14, 3/06  
 (72) 発明者; および  
 (21) 国際出願番号: PCT/JP03/03701  
 (75) 発明者/出願人 (米国についてのみ): 平野 義久 (HIRANO,Yoshihisa) [JP/JP]; 〒920-8512 石川県 金沢市 桜田町三丁目 10番地 株式会社アイ・オー・データ機器内 Ishikawa (JP). 平林 朗 (HIRABAYASHI,Akira) [JP/JP]; 〒920-8512 石川県 金沢市 桜田町三丁目 10番地 株式会社アイ・オー・データ機器内 Ishikawa (JP). 竹内 大 (TAKEUCHI,Masaru) [JP/JP]; 〒920-8512 石川県 金沢市 桜田町三丁目 10番地 株式会社アイ・オー・データ機器内 Ishikawa (JP). 安田 政昭 (YASUDA,Masaaki) [JP/JP]; 〒920-8512 石川県 金沢市 桜田町三丁目 10番地 株式会社アイ・オー・データ機器内 Ishikawa (JP).

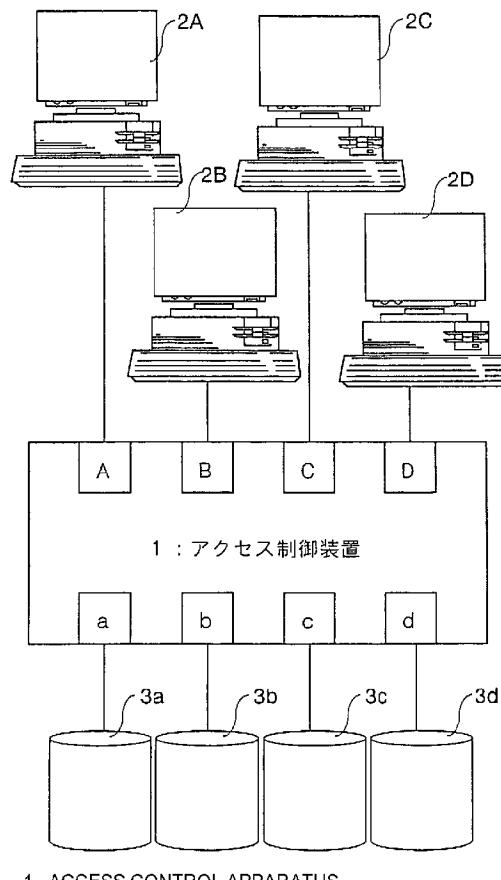
(22) 国際出願日: 2003年3月26日 (26.03.2003)  
 (25) 国際出願の言語: 日本語  
 (26) 国際公開の言語: 日本語  
 (30) 優先権データ:  
 特願2002-96049 2002年3月29日 (29.03.2002) JP  
 特願2002-136028 2002年5月10日 (10.05.2002) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社アイ・オー・データ機器 (I-O DATA DEVICE, INC.) [JP/JP]; 〒920-8512 石川県 金沢市 桜田町三丁目 10番地 Ishikawa (JP).  
 (74) 代理人: 小森 久夫 (KOMORI,Hisao); 〒540-0011 大阪府 大阪市 中央区農人橋1丁目4番34号 Osaka (JP).

[続葉有]

(54) Title: ACCESS CONTROL APPARATUS AND DATA MANAGEMENT APPARATUS

(54) 発明の名称: アクセス制御装置、およびデータ管理装置



(57) **Abstract:** An access control apparatus (1) has a plurality of interface ports (A-D) connected to external devices (2) and can set the types of permitted accesses to hard disks (3) connected to access ports (a-d) associated with the respective interface ports (A-D). Since the settings can be performed in accordance with the natures of the external devices (2) connected to the respective interface ports, shared data stored in the hard disks (3) can be prevented from being tampered or destroyed by user's operating error or intentionally.

(57) **要約:** アクセス制御装置 1 は、外部機器 2 が接続される複数のインターフェースポート A～D を有し、これらのインターフェースポート A～D 每にアクセスポート a～d に接続されるハードディスク 3 に対して許可するアクセスの種類が設定できる。したがって、インターフェースポート毎に接続される外部機器 2 の性質に応じた設定が行えるので、ユーザの誤操作や故意によりハードディスク 3 に記憶されている共有データが改竄されたり、破壊されるのを防止できる。

WO 03/083678 A1



(81) 指定国(国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:  
— 國際調査報告書

(84) 指定国(広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ヨーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許

2 文字コード及び他の略語については、定期発行される各 PCT ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

## 明細書

### アクセス制御装置、およびデータ管理装置

#### 5 技術分野

この発明は、複数のユーザで共有するデータを記憶させるハードディスク等の記憶装置に対するデータの読み出し、書き換え、書き込み、削除等の外部機器からのアクセスを制御するアクセス制御装置、およびデータ管理装置に関する。

10

#### 背景技術

従来、複数のユーザがハードディスク等の記憶装置に記憶されているデータ（以下、共有データと言う。）を利用できるように、共有データを記憶させたサーバ装置、サーバ装置に記憶されている共有データを管理する管理者用の管理装置、および共有データを利用するユーザ用の個人端末をネットワークに接続していた。また、上記共有データがユーザの誤操作等により、書き換えられたり、破壊されるのを防止するために、多くのネットワークシステムではユーザに対して共有データの書換、書込、および削除を禁止し、共有データの読出（ダウンロード）のみ許可している。特に、インターネット上で共有データを公開しているサーバ装置の場合、不特定多数のユーザからアクセスがあるため、ユーザに対して共有データの書換、書込、および削除を禁止している場合が多い。例えば、サーバ装置に対して共有データの書換、書込、および削除を行う場合、パスワード等による認証（記憶装置に対して共有データの書換、書込、削除が許可されている者（共有データの管理者）であるかどうかの認証）を行うことで、パスワードを知らない者（ユーザ）に対して共有データの書換、書込、および削除を禁止していた。

なお、ユーザは共有データの書換、書込、および削除を行う必要性はなく、サーバ装置から共有データをダウンロードして利用できればよい。

また、ここで言う、書換とはサーバ装置に記憶されている共有データの変更／更新であり、書込とはサーバ装置に新たな共有データを追加する

5 ことである。

しかしながら、サーバ装置に記憶している共有データを改竄したり（故意に書き換えたり）、破壊する犯罪（ハッカーによる犯罪）が増加しており、上記パスワード等による認証で共有データの書換、書込、削除を許可する方式では、共有データのセキュリティが低いという問題があった。

10 また、ユーザが記憶装置から読み出した共有データを利用すると、該利用にともなって新たな共有データが生まれたり、記憶装置に記憶されている共有データに変更が生じる環境で運用されているネットワークシステムがある。例えば、病院では各患者のカルテを記憶装置に記憶させたカルテシステムが利用されている。カルテシステムは、医師（カルテシステムのユーザ）が患者に対して適正な医療行為を行うためのシステムである。

医師は、記憶装置から該当患者のカルテを読み出し、該患者に対するこれまでの診療履歴を確認し、患者に対する今回の医療行為の内容を判断している。医師は、患者に対する今回の医療行為が完了すると、記憶装置に記憶されている該患者のカルテを、今回の医療行為の内容を追加したカルテに置き換えるなければならない。このため、医師に対してカルテ（共有データ）の書換を許可しないネットワークシステムでカルテシステムを構成すると、医師が患者に対して行った医療行為の内容を該患者のカルテに登録できない。この場合、患者に対して、同じ医療行為が重複して行われる等、医療行為が適正に行えず、医療事故が発生する可能性が高くなる。このため、カルテシステムは、医師に対して共有データである患者のカルテの書換を許可したネットワークシステムで構成されていた。

このように、記憶装置に記憶されている共有データの書換をユーザに

許可した環境で運用されているネットワークシステムも多く、このような環境で運用されているネットワークシステムでは、ユーザの誤操作による共有データの無用な書き換えや、悪意を持った者による共有データの改竄から、共有データが十分に保護されていなかった。

5 この発明の目的は、ユーザの誤操作や故意により、記憶装置に記憶しているデータが改竄されたり、破壊されるのを防止することにより、上記データのセキュリティを向上させたアクセス制御装置、およびデータ管理装置を提供することにある。

## 10 発明の開示

この発明のアクセス制御装置は、  
外部機器が接続される複数のインターフェースポートと、  
データを記憶する記憶装置が接続されるアクセスポートと、  
上記インターフェースポート毎に、上記記憶装置に対して許可するア  
クセスの種類を設定し、上記記憶装置に対するアクセスの要求がいずれかの  
15 インタフェースポートに入力されたとき、該インターフェースポートに対して許可されているアクセスの種類に基づいて、入力されたアクセスの要求の実行可否を判断する制御部と、を備えている。

この構成では、制御部において、外部機器が接続されるインターフェー  
20 スポート毎に、アクセスポートに接続されている記憶装置に対して許可す  
るアクセスの種類が設定される。ここで言う外部機器とは、記憶装置に記  
憶されているデータ（共有データ）を利用するユーザが操作する個人端末  
や、記憶装置に記憶されている共有データを管理する管理者が操作する管  
理装置である。

25 上記アクセスの種類は、例えば、  
①記憶装置が記憶している共有データの読み出し、  
②記憶装置が記憶している共有データの書き換え、

③記憶装置に対する共有データの書き込み、

④記憶装置が記憶している共有データの削除、

である。上記制御部は、インターフェースポート毎に、上記①～④の1つ、または複数について許可する設定を行う。

5 また、上記制御部は、上記記憶装置に対するアクセスの要求がいずれかのインターフェースポートに入力されたとき、該インターフェースポートに対して許可されているアクセスの種類に基づいて入力されたアクセスの要求の実行可否を判断する。

10 例えは、許可されているアクセスの種類が、上記①のみであるインターフェースポートにおいて、入力されたアクセスの要求が上記①であれば、このアクセスの要求について実行可と判断する。一方、該インターフェースポートにおいて入力されたアクセスの要求が上記②～④であれば、入力された要求について実行不可と判断する。このため、記憶装置に記憶されている共有データをダウンロードのみ許可するユーザについては、該ユーザが接続するインターフェースポートに対して共有データの読出のみ許可する設定としておけば、該インターフェースポートに接続したユーザの誤操作や、故意により記憶装置に記憶されている共有データが改竄されたり、破壊されるのを防止することができる。

15 また、各インターフェースポートに対して許可するアクセスの種類の設定については、装置本体における操作で設定できるように構成し、外部機器からの遠隔操作で設定できないように構成することにより、セキュリティの一層の向上が図れる。

20 また、共有データを管理する管理者が操作する装置（外部機器）が接続されるインターフェースポートについては、上記①～④の全てを許可する設定にしておくことにより、管理者における共有データの管理が面倒になるということもない。また、インターフェースポートに対して、上記①と③とを許可すると、該インターフェースポートに接続したユーザは共有データ

の読み出だけでなく、共有データの追加も行える。この設定であれば、共有データをユーザに見せて、該共有データに対する感想をユーザから入手し、これを新たな共有データとする等のシステムとして利用でき、また、該設定のインターフェースポートに接続したユーザは共有データの書換や、削除を行うことができないので、共有データに対するセキュリティも十分に確保することができる。

さらに、各インターフェースポートは、上記①～④の1つ以上を許可した設定にできるので、該インターフェースポートに接続されるユーザの性質に応じた設定が行え、多様な用途に対応しながら、共有データのセキュリティを十分に確保することができる。

この発明は、また、

外部機器が接続されるインターフェースポートと、

データを記憶する記憶装置が接続される複数のアクセスポートと、

上記アクセスポート毎に、接続されている上記記憶装置に対して許可するアクセスの種類を設定し、いずれかのアクセスポートに接続されている上記記憶装置に対するアクセスの要求が上記インターフェースポートに入力されたとき、アクセスが要求された上記記憶装置が接続されている上記アクセスポートに対して許可されているアクセスの種類に基づいて、入力されたアクセスの要求の実行可否を判断する制御部と、を備えている。

この構成では、制御部がアクセスポート毎に接続されている記憶装置に対して許可するアクセスの種類（上記で説明した①～④）を設定する。

また、制御部は、インターフェースポートにおいて、いずれかのアクセスポートに接続されている記憶装置に対するアクセスの要求があると、該アクセスポートに対して許可されているアクセスの種類に基づいて、入力されたアクセスの要求の実行可否を判断する。

例えば、許可されているアクセスの種類が、上記①のみであるアクセスポートに接続されている記憶装置に対して、入力されたアクセスの要求

が上記①であれば、このアクセスの要求について実行可と判断する。一方、該アクセスポートに接続されている記憶装置に対して入力されたアクセスの要求が上記②～④であれば、入力された要求について実行不可と判断する。

5 このように、アクセスポート毎に接続されている記憶装置に対して許可するアクセスの種類を設定することができるので、記憶装置に記憶されている共有データの性質、例えば共有データをユーザに見せて、該共有データに対する感想をユーザから入手するシステムであれば、ユーザに対して提示する共有データを記憶する記憶装置、入手したユーザの感想を記憶する記憶装置等、に応じてアクセスを許可する種類を設定することができる。

10 なお、ユーザに対して提示する共有データを記憶する記憶装置が接続されるアクセスポートについては共有データの読み出しのみ許可すればよく、また、入手したユーザの感想を記憶する記憶装置が接続されるアクセスポートについては共有データの書き込みのみ許可すればよい。

15 この発明は、また、

外部機器が接続されるインターフェースポートと、

記憶装置が接続されるアクセスポートと、

20 上記アクセスポートに接続された上記記憶装置に対して許可するアクセスの種類をデータの読み出しおよび新規書き込みに設定し、上記インターフェースポートに入力された上記記憶装置に対するアクセスの要求が、データの読み出しありは新規書き込みのいずれかであれば入力されたアクセスの要求を実行し、データファイルの読み出しありは新規書き込み以外の要求であれば入力されたアクセスの要求を無視する制御部と、を備えている。

25 この構成では、データを記憶する記憶装置、例えばハードディスク、がアクセスポートに接続され、この記憶装置に記憶されているデータを利用する外部機器がインターフェースポートに接続される。制御部は、インタ

フェースポートに接続された外部機器から、データの読出、または新規書込の要求があれば該要求を実行するが、インターフェースポートに接続された外部機器から、上記データの読出、または新規書込以外の要求である、例えばデータの書換（上書き）または削除の要求があっても、この要求を  
5 無視する。

したがって、アクセスポートに接続された記憶装置に記憶されたデータを、書き換えたり、削除することはできない。これにより、アクセスポートに接続された記憶装置に記憶されたデータは、ユーザの誤操作による無用な書き換えや、悪意を持った者による改竄から、十分に保護できる。

10 また、インターフェースポートに記憶装置に対するデータの新規書込の要求が入力されると該要求を実行するので、ユーザが記憶装置に記憶されているデータの更新を行う必要がある環境で使用されるシステムであっても、新たに発生したデータを記憶装置に新規に書き込むことにより、更新されたデータを記憶装置に記憶させることができる。

15

### 図面の簡単な説明

図1は、この発明の実施形態であるアクセス制御装置を適用したネットワークシステムの構成を示す図である。

20 図2は、この発明の実施形態であるアクセス制御装置の構成を示す図である。図3は、この発明の実施形態であるアクセス制御装置の動作を示すフローチャートである。

図4は、この発明の実施形態であるアクセス制御装置における共有データの読出処理を示すフローチャートである。

25 図5は、この発明の実施形態であるアクセス制御装置における共有データの書換処理を示すフローチャートである。

図6は、この発明の実施形態であるアクセス制御装置における共有データの書込処理を示すフローチャートである。

図7は、この発明の実施形態であるアクセス制御装置における共有データの削除処理を示すフローチャートである。

図8は、この発明の実施形態であるアクセス制御装置をインターネットに適用した例を示す図である。

5 図9は、この発明の別の実施形態であるアクセス制御装置における共有データの読み出し処理を示すフローチャートである。

図10は、インターフェースポートA～D毎に、且つアクセスポートa～d毎に許可するアクセスの種類を設定する方法を説明する図である。

10 図11は、この発明のさらに他の実施形態であるアクセス制御装置を適用したネットワークシステムを示す図である。

図12は、この発明のさらに他の実施形態であるアクセス制御装置の構成を示す図である。

図13は、カルテのファイルネームを示す図。

15 図14は、この発明のさらに他の実施形態であるアクセス制御装置の動作を示すフローチャートである。

図15は、この発明のさらに他の実施形態アクセス制御装置の動作を示すフローチャートである。

### 発明を実施するための最良の形態

20 以下、この発明の実施形態であるアクセス制御装置について詳細に説明する。

図1は、この発明の実施形態であるアクセス制御装置を適用したネットワークシステムを示す図である。図において、1はこの発明の実施形態であるアクセス制御装置である。アクセス制御装置1は、外部機器2（25 A～2D）が接続される複数（この実施形態では4つ）のインターフェースポートA～Dと、ハードディスク3（3a～3d）（この発明で言う記憶装置）が接続される複数（この実施形態では4つ）のアクセスポートa

～dとを有している。外部機器2は、共有データを利用するユーザの個人端末や、記憶装置3に記憶されている共有データを管理する管理者用の管理装置である。外部機器2は、パーソナルコンピュータや、携帯端末等、データ通信機能を有する装置であれば特にその種類は制限されない。アクセス制御装置1と外部機器2とは、直接ケーブルで接続される構成であってもよいし、またLANやインターネット等のネットワークを介して接続される構成であってもよい。アクセス制御装置1とハードディスク3により、サーバ装置が構成される。サーバ装置は、アクセス制御装置1とハードディスク3とは、一体化された構成であってもよい。

図2は、この発明の実施形態であるアクセス制御装置の構成を示す図である。アクセス制御装置1は、本体の動作を制御する制御部11と、外部機器2が接続されるインターフェースポートA～D毎に、入出力を制御するインターフェースコントローラ12（12A～12D）と、インターフェースポートA～D毎に入出力されるデータを一時的に記憶するFIFO13（13A～13D）と、キャッシュメモリ14を制御するキャッシュコントローラ15と、ハードディスク3が接続されるアクセスポートa～d毎に入出力されるデータを一時的に記憶するFIFO16（16a～16d）と、各アクセスポートa～dに接続されているハードディスク3（3a～3d）を制御するデバイスコントローラ17と、を備えている。インターフェースコントローラ12は、SCSIやIDE等のインターフェースにより他の装置（外部機器）との接続を制御する。デバイスコントローラ17は、アクセスポートa～dに接続されているハードディスク3に対するデータの読み出しや、書き込みを制御する。

アクセス制御装置1は、インターフェースポートA～D毎にアクセスポートa～dに接続されているハードディスク3に対して許可するアクセスの種類を設定している。この設定は、アクセス制御装置1に設けられている操作部（不図示）においてのみ変更可能であり、インターフェースポート

A～Dに接続されている外部機器2から変更できないように構成されている。

各インターフェースポートA～Dには、

- ①ハードディスク3が記憶している共有データの読み出し、  
5 ②ハードディスク3が記憶している共有データの書き換え（記憶している共有データの変更）、

③ハードディスク3に対する新たな共有データの書き込み、

④ハードディスク3が記憶している共有データの削除、

の1つ、または複数について許可する設定がなされる。各インターフェースコントローラ12は、ハードディスク3に対するアクセスの要求が入力されたとき、該アクセスの種類が上記制御部11により許可されている種類であるかどうかを判断し、許可されていると判断した場合に該要求を受け付け、反対に許可されていないと判断した場合に該要求を拒否する。

この実施形態では、インターフェースポートAは共有データの読み出しのみ許可した設定であり、インターフェースポートBは共有データの読み出し、および共有データの書き換えを許可した設定であり、インターフェースポートCは共有データの読み出し、および共有データの書き込みを許可した設定であり、インターフェースポートDは共有データの読み出し、共有データの書き換え、共有データの書き込み、および共有データの削除を許可した設定である、場合を例にする。

共有データをダウンロードして利用するだけのユーザ（一般ユーザ）の個人端末（外部機器2A）は、インターフェースポートAに接続される。また、共有データをダウンロードして利用するだけでなく、必要に応じて共有データを書き換えるユーザは、インターフェースポートBに接続される。また、共有データをダウンロードして利用するだけでなく、必要に応じて新たな共有データを書き込むユーザは、インターフェースポートCに接続される。さらに、共有データの読み出、書換、書込、削除を必要に応じて行

う共有データの管理者は、インターフェースポートDに接続される。

また、アクセスポートa～dに接続した4つのハードディスクにより、RAIDレベル0／1のシステムを構成している。具体的には、アクセスポートa、bに接続されている2つのハードディスク3a、3bが共有データを記憶するデータ記憶用として機能し、アクセスポートc、dに接続されている2つのハードディスク3c、3dが、それぞれアクセスポートa、bに接続されているハードディスク3のミラーリング用として機能する。また、所定の大きさのブロックに分割した共有データを、アクセスポートa、bに接続されている2つのハードディスク3a、3bに記憶している。具体的には、奇数番目のブロックをハードディスク3aに記憶し、偶数番目のブロックをハードディスク3bに記憶している。

なお、ミラーリング用であるハードディスク3cは奇数番目のブロックを記憶しており、ハードディスク3dは偶数番目のブロックを記憶している。

ハードディスク3cはハードディスク3aのバックアップ用として機能し、ハードディスク3dはハードディスク3bのバックアップ用として機能する。

デバイスコントローラ17は、共有データの書き換え、または書き込みを行う場合、書き換える共有データ、または書き込む共有データを所定の大きさのブロックに分割し、アクセスポートa、bに接続されているハードディスク3a、3bに書き込む。また、このときアクセスポートc、dに接続されているハードディスク3c、3dにも所定の大きさのブロックに分割した共有データを書き込む。ハードディスク3a、3cに書き込まれる共有データは同じブロックであり、ハードディスク3b、3dに書き込まれる共有データは同じブロックである。また、デバイスコントローラ17は、共有データを削除する場合、アクセスポートa～dに接続されているハードディスク3a～3dにおいて、該当する共有データが記憶さ

5 れている領域を空き領域に設定する。さらに、デバイスコントローラ 17 は、共有データを読み出す場合、アクセスポート a に接続されているハードディスク 3a から所定の大きさのブロック単位に分割された奇数番目のデータを読み出し、且つアクセスポート b に接続されているハードディスク 3b から所定の大きさのブロック単位に分割された偶数番目のデータを読み出し、これらを順番に並べることにより共有データを作成する（所定の大きさのブロックに分割されていた共有データを一体化する。）。

以下、この実施形態のアクセス制御装置 1 の動作について説明する。

10 図 3 は、アクセス制御装置の動作を示すフローチャートである。各インターフェースコントローラ 12A～12D は、それぞれが独立してアクセスポート a～d に接続されているハードディスク 3 に対するアクセスの要求がインターフェースポート A～D に入力されるのを待っている（s1）。インターフェースポート A～D に入力されるアクセスの要求は、共有データの読み出、書換、書込、または削除である。

15 12 インタフェースコントローラ 12 は、ハードディスク 3 に対するアクセスの要求が接続されているインターフェースポートに入力されると、該アクセスの要求が接続されているインターフェースポートに対して許可されている種類であるかどうかを判断する（s2）。インターフェースコントローラ 12 は、s2 でアクセスの要求が許可されている種類であると判断すると、該要求に基づく処理を実行する（s3）。反対に、s2 で許可されていない種類であると判定すると、該アクセスの要求を送信してきた外部機器 2 に対してエラーコマンドを送信する（s4）。

アクセス制御装置 1 は、s3、または s4 の処理を完了すると、s1 に戻って上記処理を繰り返す。

25 このように、この実施形態のアクセス制御装置 1 は、インターフェースポート毎に許可するアクセスの種類が設定されており、許可されていない種類のアクセスの要求が入力された場合に、該アクセスの要求を拒否する

。したがって、インターフェースポートに接続される外部機器2の性質に応じた設定が行える。例えば、ハードディスク3に記憶している共有データをダウンロードして利用するだけのユーザの外部機器2を接続するインターフェースポートについては、共有データの読み出しのみ許可する設定にしておけば、このユーザの誤操作や故意により共有データが改竄されたり、破壊されるのを防止することができる。これにより、共有データのセキュリティを向上させることができる。

なお、上記ユーザは共有データをダウンロードして利用するだけであるので、共有データの書換、書き込み、削除を禁止しても問題はない。

また、インターフェースポートCのように、共有データの読み出し、および書き込みを許可したインターフェースポートを設けることにより、ユーザに共有データを提示し、該提示した共有データに対する感想をユーザから入手するアンケート方式等に対応することができる。但し、このインターフェースポートCに接続される外部機器2についても共有データの書換、削除については、そのアクセスの要求を拒否するので、ユーザの誤操作や故意により共有データが改竄されたり、破壊されるのを防止することができる。

さらに、インターフェースポートDのように、共有データの読み出し、書換、書き込み、および削除を許可したインターフェースポートについては、共有データを管理する管理者の外部機器2を接続すればよい。これにより、管理者はハードディスク3に記憶されている共有データの管理がスムーズに行える。

なお、共有データの書換や、削除時にパスワードによる認証を行えば、共有データのセキュリティを一層向上させることができる。反対に上記パスワードによる認証を無くせば、共有データの書換や、削除を行うときの作業性を向上させることができる。

上記S3で実行される処理は、共有データの読み出し、変更、追加、削除のいずれかである。図4は、共有データの読み出し処理を示すフローチャート

である。アクセスの要求が入力されたインターフェースコントローラ12は、キャッシュコントローラ15に対して共有データの読み出しが転送する(s11)。この読み出しがあるには、読み出す共有データを特定するためのデータが含まれている。

5 キャッシュコントローラ15は、転送されてきた上記読み出しがより要求されている共有データ(該当する共有データ)がキャッシュメモリ14に記憶されているかどうかを判定する(s12)。キャッシュコントローラ15は、s12でキャッシュメモリに該当する共有データが記憶されていると判定すると、該読み出しが送信してきたインターフェースコントローラ12A~12Dに対して共有データの読み出し完了を通知する(s15)。反対に、s12でキャッシュメモリに記憶されていないと判定すると、デバイスコントローラ17に対して、該当する共有データの読み出しを指示する(s13)。

15 共有データの読み出しが指示されたデバイスコントローラ17は、アクセスポートa、bに接続されているハードディスク3a、3bから、該当する共有データを読み出し、キャッシュメモリ14に書き込む(s14)。

1 上述したように、共有データは所定の大きさのブロックに分割され、  
2 アクセスポートaに接続されているハードディスク3aに奇数番目のデータが記憶され、  
3 アクセスポートbに接続されているハードディスク3bに偶数番目のデータが記憶されている。ハードディスク3a、3bから読み出された共有データは一旦FIFO16a、16bに記憶される。デバイスコントローラ17は、FIFO16a、16bから交互に、記憶されている共有データを取り出し、取り出した順番にキャッシュメモリ14に書き込む。これにより、ハードディスク3a、3bに所定の大きさのブロックに分割されて記憶されていた共有データを一体化する(適正な共有データを作成する)。また、ハードディスク3a、3bから同時に共有データ

タを読み出すので、共有データを分割せずに单一のハードディスクに記憶させている場合に比べて、ハードディスク3に記憶されている共有データの読み出しにかかる時間が約半分になる。

デバイスコントローラ17は、該当する共有データの読み出しを完了すると、その旨をキャッシュコントローラ15に通知する(s15)。

キャッシュコントローラ15は、デバイスコントローラ17から該当する共有データの読み出し完了が通知されると、今回共有データの読出要求を転送してきたインターフェースコントローラ12に対して、該読出完了を転送する(s16)。また、キャッシュコントローラ15は、キャッシュメモリ14に記憶されている該当する共有データをインターフェースコントローラ12に転送する(s17)。キャッシュコントローラ15は、s17においてキャッシュメモリ14に記憶されている該当する共有データを順次読み出しFIFO13に記録する。

キャッシュコントローラ15から共有データの読出完了が転送されたインターフェースコントローラ12は、FIFO13に記憶されている共有データを順番に読み出し、今回ハードディスク3に対してアクセス(共有データの読出)を要求してきた外部機器2に対してインターフェースポートから共有データを出力する(s18)。

これにより、共有データの読み出しが許可されているインターフェースポートに接続されている外部機器2では、共有データをダウンロードして利用することができる。

次に、s3で実行される共有データの書換処理について説明する。図5は、共有データの書換処理を示すフローチャートである。インターフェースコントローラ12は、キャッシュコントローラ15に対して共有データの書換要求を転送する(s21)。この書換要求には、書き換える共有データを特定するためのデータが含まれている。また、インターフェースコントローラ12は、共有データの書換要求とともに外部機器2から送信され

てきた書き換える共有データをFIFO13に書き込んでいく(s22)

。

キャッシュコントローラ15は、キャッシュメモリ14に空き領域を確保し(s23)、書き換える共有データをFIFO13から読み出し、

5 ここで確保した空き領域に記憶する(s24)。キャッシュコントローラ15は、書き換える共有データをキャッシュメモリ14に記憶すると、デバイスコントローラ17に対して共有データの書換を指示する(s25)

。

キャッシュコントローラ15から共有データの書換指示があったデバイスコントローラ17は、アクセスポートa～dに接続されている4つのハードディスク3a～3dに対して共有データの書換を指示する(s26)。また、デバイスコントローラ17は、キャッシュメモリ14に記憶されている該当する共有データ(書き換える共有データ)を読み出、所定のブロック単位に分割した共有データをFIFO16a、16bに書き込んで行く。このとき、デバイスコントローラ17は、FIFO16aに書き込んだデータと同じデータをFIFO16cに書き込んでおり、またFIFO16bに書き込んだデータと同じデータをFIFO16dに書き込んでいる。

20 ハードディスク3a～3dは、それぞれFIFO16a～16dに記憶されている共有データを取り込んで、該当する共有データを書き換える(s27)。

次に、s3で実行される共有データの書込処理について説明する。図6は、共有データの書込処理を示すフローチャートである。アクセスの要求が入力されたインターフェースコントローラ12は、キャッシュコントローラ15に対して共有データの書込要求を転送する(s31)。この書込要求には、ハードディスク3に書き込む共有データが含まれている。また、インターフェースコントローラ12は、共有データの書込要求とともに外

部機器 2 から送信されてきたハードディスク 3 に書き込む共有データを FIFO 13 に書き込んでいく (s 3 2)。

キャッシュコントローラ 15 は、キャッシュメモリ 14 に空き領域を確保し (s 3 3)、書き込む共有データを FIFO 13 から読み出し、ここで確保した空き領域に記憶する (s 3 4)。キャッシュコントローラ 15 は、書き込む共有データをキャッシュメモリ 14 に記憶すると、デバイスコントローラ 17 に対して共有データの書き込みを指示する (s 3 5)。

キャッシュコントローラ 15 から共有データの書き込み指示があったデバイスコントローラ 17 は、アクセスポート a～d に接続されている 4 つのハードディスク 3 a～3 d に対して共有データの書き込みを指示する (s 3 6)。また、デバイスコントローラ 17 は、キャッシュメモリ 14 に記憶されている該当する共有データ（書き込む共有データ）を読み出、所定の大きさのブロックに分割し、奇数番目のブロックのデータを FIFO 16 a に書き込み、偶数番目のブロックのデータを FIFO 16 b に書き込む。このとき、デバイスコントローラ 17 は、FIFO 16 a に書き込んだデータと同じデータを FIFO 16 c に書き込んでおり、また FIFO 16 b に書き込んだデータと同じデータを FIFO 16 d に書き込んでいる。

ハードディスク 3 a～3 d は、それぞれ FIFO 16 a～16 d に記憶されている共有データを取り込んで、空き領域に該当する共有データを書き込む (s 3 7)。

この共有データの書き込みにかかる時間は、共有データを分割せずに单一のハードディスクに記憶させる場合に比べれば略半分で済む。

さらに、s 3 で実行される共有データの削除処理について説明する。

図 7 は、共有データの削除処理を示すフローチャートである。アクセスの要求が入力されたインターフェースコントローラ 12 は、キャッシュコント

ローラ 1 5 に対して共有データの削除要求を転送する (s 4 1)。この削除要求には、削除する共有データを特定するためのデータが含まれている。

5 キャッシュコントローラ 1 5 は、インターフェースコントローラ 1 2 から転送されてきた削除要求を、デバイスコントローラ 1 7 に転送する (s 4 2)。

デバイスコントローラ 1 7 は、ハードディスク 3 a ~ 3 d に対して、この削除要求で指示されている共有データの削除を指示する (s 4 3)。

10 ハードディスク 3 a ~ 3 d は、今回削除が指示された共有データを記憶している記憶領域を空き領域にすることで、指示された共有データを削除する。ここで空き領域とした領域（削除した共有データを記憶していた領域）は、上記書き込み処理において共有データを書き込む領域として利用される。

15 このように、アクセスポート a ~ d に接続される 4 つのハードディスク 3 a ~ 3 d で RAID レベル 0 / 1 を構成したので、共有データの読み出、書き換、および書き込みを高速に行うことができる。また、いずれかのハードディスク 3 a ~ 3 d が故障しても、故障したハードディスクに記憶されていた共有データが別のハードディスクに記憶されているので、共有データが消失することがない。

20 なお、上記実施形態ではアクセスポート a ~ d に接続される 4 つのハードディスク 3 a ~ 3 d で RAID レベル 0 / 1 を構成するとしたが、これに限定されることはなく、RAID レベルは別のレベルであってもよいし、また RAID を構成しなくてもよい。

25 次に、上記実施形態のアクセス制御装置 1 とハードディスク 3 とを一体化したデータ管理装置 1、3 を、インターネット上で共有データを公開するシステムに適用した実施形態について説明する。図 8 は、この実施形態にかかるシステムの構成を示す図である。インターネット 2 1 を介して共有

データをダウンロードするユーザの個人端末 2 A（外部機器 2 A）は、Web サーバ 2 3 を介して上記共有データの読出のみ許可されたデータ管理装置 1、3 のインターフェースポート A に接続されている。また、上記共有データの読出、書換、書込、および削除が許可されたインターフェースポート D には、インターネット 2 2 に接続された管理者の管理サーバ装置 2 4 が接続されている。共有データの管理者が操作する管理装置 2 D（外部機器 2 D）は、上記インターネット 2 2 に接続されており、管理サーバ装置 2 4 を介してデータ管理装置 1、3 にアクセスする。

ユーザは、インターネット 2 1、Web サーバ 2 3 を介してデータ管理装置 1、3 にアクセスし、共有データのダウンロード（読出）を要求する。ユーザが操作する個人端末 2 A から出力されたデータ管理装置 1、3 へのアクセスの要求は、インターフェースポート A に入力されるので、上述したようにユーザは共有データをダウンロードし利用することができる。一方、ユーザは共有データの書換、書込、削除については、データ管理装置 1、3 に要求しても拒否される。したがって、インターネット 2 1 を介して接続されるユーザの誤操作や故意により共有データが改竄されたり、破壊されるのを防止することができる。

また、共有データを管理する管理者用の管理装置 2 D は、インターネット 2 2、管理サーバ装置 2 4 を介してデータ管理装置 1、3 に設けられたインターフェースポート D（共有データの読出、書換、書込、および削除が許可されたインターフェースポート）に接続される。このため、管理者は、データ管理装置 1、3 で管理されている共有データの読出、書換、書込、および削除が行える。したがって、管理者は共有データをスムーズに管理することができる。

なお、管理者はインターネット 2 2 に接続されている、いずれかの管理装置 2 D において、共有データの読出、書換、書込、および削除を行えばよい。

また、ユーザが操作する個人端末 2 A が接続されるインターフェースポート（Web サーバ 2 3 が接続されるインターフェースポート）に対して、共有データの読出、および書込を許可しておけば、共有データをダウンロードしたユーザから、該ダウンロードした共有データに対する感想を新たな共有データとして入手することができる。これにより、インターネット 2 1、Web サーバ 2 3 を介してデータ管理装置 1、3 に接続した複数人のユーザが対話するシステムや、ユーザに対してアンケートを行うシステム等、様々なシステムを構築することができる。しかも、インターネット 2 1 を介して接続されるユーザの個人端末 2 は共有データの書換、および削除については許可されないので、インターネット 2 1 を介して接続されるユーザの誤操作や故意により共有データが改竄されたり、破壊されるのを防止することができる。

このように、この実施形態のアクセス制御装置 1 は、外部機器 2 が接続されるインターフェースポート毎に許可するアクセスの種類を設定する構成としたので、多様な用途に対応することができ、且つ共有データのセキュリティを十分に確保することができる。

次に、この発明の別の実施形態について説明する。

上記実施形態では、インターフェースポート A～D 每にハードディスク 3 a～3 d に対して許可するアクセスの種類を設定するとしたが、この実施形態ではアクセスポート a～d 每に接続されているハードディスク 3 a～3 d に対して許可するアクセスの種類を設定するようにした実施形態である。

ここでは、

- ①アクセスポート a に接続されているハードディスク 3 a については、  
25 共有データの読出のみ許可する設定とし、
- ②アクセスポート b に接続されているハードディスク 3 b については、  
共有データの書換のみ許可する設定とし、

③アクセスポート c に接続されているハードディスク 3 c については、共有データの書込み許可する設定とし、

④アクセスポート d に接続されているハードディスク 3 d については、共有データの読み出、書換、書込み、および削除を拒否する設定とする。

5 なお、アクセスポート c に接続されているハードディスク 3 c は、アクセスポート a に接続されているハードディスク 3 a のバックアップ用である。

図 9 は、この実施形態のアクセス制御装置の動作を示すフローチャートである。各インターフェースコントローラ 12 A～12 D は、アクセスポート a～d に接続されているハードディスク 3 に対するアクセスの要求がインターフェースポート A～D に入力されるのを待っている (s 5 1)。インターフェースポート A～D に入力されるアクセスの要求は、共有データの読み出、書換、書込み、または削除である。

15 インターフェースコントローラ 12 は、接続されているインターフェースポートに入力されたアクセスの要求が、共有データの読み出、書換、書込み、または削除のどれであるかを判定する (s 5 2～s 5 4)。読み出であると判定すると、共有データの読み出処理をアクセスポート a に接続されているハードディスク 3 a に対して実行する (s 5 5)。また、書換であると判定すると、共有データの書換処理をアクセスポート b に接続されているハードディスク 3 b に対して実行する (s 5 6)。さらに、書込みであると判定すると、共有データの書込み処理をアクセスポート c に接続されているハードディスク 3 c に対して実行する (s 5 7)。一方、削除であると判定した場合 (読み出、書換、書込みのいずれでもないと判定した場合)、該アクセスの要求を送信してきた外部機器 2 に対してエラーコマンドを送信する (s 5 8)。

s 5 5、s 5 6、s 5 7 の処理は、それぞれ図 4、5、6 に示した処理と略同じ処理であるので、ここでは詳細な説明は省略する。共有データ

の読み出、書換、書き込みを単一のハードディスク 3 に対して行う点で相違するだけである。

5 このように、この実施形態のアクセス制御装置 1 によれば、共有データの書換や、書き込みが行われるハードディスクを特定したので、ユーザの誤操作や故意による共有データの改竄や、破壊が行われても、ハードディスク 3 a に共有データが残っているので問題がない。また、ハードディスク 3 a が故障しても、ハードディスク 3 d に共有データがバックアップされているので、共有データが消失することもない。

10 また、インターフェースポート A～D 毎に、各ハードディスク 3 (各アクセスポート a～d に接続されているハードディスク 3) に許可するアクセスの種類がそれぞれ設定できるように構成してもよい。例えば、テープルを利用してインターフェースポート A～D 毎に、各ハードディスク 3 に許可するアクセスの種類をそれぞれ設定する (図 10 参照)。これにより、例えば、

15 ①インターフェースポート A について、

アクセスポート a に接続されているハードディスク 3 a に対し共有データの読み出のみ許可し、

アクセスポート b、c、d 接続されているハードディスク 3 b、3 c、3 d に対し全てのアクセスを許可しない設定にする。

20 ②インターフェースポート B について、

アクセスポート a に接続されているハードディスク 3 a に対し共有データの読み出のみ許可し、

アクセスポート b に接続されているハードディスク 3 b に対し共有データの書換のみ許可し、

25 アクセスポート c に接続されているハードディスク 3 c に対し共有データの書き込みのみ許可し、

アクセスポート d に接続されているハードディスク 3 d に対し全てのア

クセスを許可しない設定にする。

③インターフェースポートCについて、

アクセスポートaに接続されているハードディスク3aに対し共有データの書換のみ許可し、

5 アクセスポートbに接続されているハードディスク3bに対し共有データの書き込み、および書換のみ許可し、

アクセスポートcに接続されているハードディスク3cに対し共有データの読み出しのみ許可し、

アクセスポートdに接続されているハードディスク3dに対し全てのア  
10 クセスを許可しない設定にする。

④インターフェースポートDについて、

アクセスポートaに接続されているハードディスク3aに対して共有データの書き込みのみ許可し、

15 アクセスポートbに接続されているハードディスク3bに対し共有データの読み出しのみ許可し、

アクセスポートcに接続されているハードディスク3cに対し共有データの書換のみ許可し、

アクセスポートdに接続されているハードディスク3dに対し全てのア  
クセスを許可しない設定にする。

20 このように、インターフェースポートA～D毎に、各アクセスポートa～dに接続されているハードディスク3に対して許可するアクセスの種類をそれぞれ設定することができる。これにより、各インターフェースポートA～Dに接続される外部機器2の性質と、各アクセスポートa～dに接続されるハードディスク3の性質と、に応じた設定が行える。これにより、  
25 多様なシステムに対応することができ、且つハードディスク3に記憶されている共有データのセキュリティも十分に確保することができる。

図11は、この発明のさらに他の実施形態であるアクセス制御装置を

適用したネットワークシステムを示す図である。

図において、アクセス制御装置1は、サーバ装置6（6A、6B）が接続される複数（この実施形態では2つ）のインターフェースポートA、Bと、ハードディスク3（3a～3d）（この発明で言う記憶装置）が接続される複数（この実施形態では4つ）のアクセスポートa～dとを有している。ハードディスク3には、各患者のカルテが記憶されている。

なお、この発明で言うデータ記憶装置は、アクセス制御装置1とハードディスク3a～3dとを一体的に構成したものである。

インターフェースポートAは、アクセスポートa～dに接続されている  
10 ハードディスク3に対してデータ（患者のカルテ）の読み出しが許可されており、ハードディスク3に対するデータの新規書き込み、書き換（上書き）、削除については許可されていない。また、インターフェースポートBは、アクセスポートa～dに接続されているハードディスク3に対するデータ（患者のカルテ）の新規書き込みが許可されたポートであり、ハードディスク3  
15 に対してデータの読み出しが許可されていない。

インターフェースポートAに接続されているサーバ装置6Aは、アクセスポートa～dに接続されているハードディスク3に記憶されているデータの読み出しが制御するサーバ装置である。インターフェースポートBに接続されているサーバ装置6Bは、アクセスポートa～dに接続されているハードディスク3a～3dに対するデータの新規書き込みを制御するサーバ装置である。

また、図11に示す4はLAN等のネットワークであり、5はネットワーク4に接続されたパーソナルコンピュータ等の端末装置である。端末装置5は、ハードディスク3に記憶されているカルテを読み出して利用するユーザが操作する外部機器である。端末装置5は、サーバ装置6Aおよびサーバ装置6Bの両方に同時に接続することはできないが、選択的にどちらか一方に接続できる。端末装置5を操作するユーザは、ハードディス

ク3に記憶されているカルテを読み出すときにサーバ装置6Aに接続し、ハードディスク3にカルテを書き込むときにサーバ装置6Bに接続する。

なお、この実施形態では端末装置5は、サーバ装置6A、6Bを介してアクセス制御装置1のインターフェースポートに接続されるとしているが5、サーバ装置6A、6Bを介さずに直接アクセス制御装置1のインターフェースポートA、Bに接続されるように構成にしてもよい。

図12は、この発明の実施形態であるアクセス制御装置の構成を示す図である。アクセス制御装置1は、本体の動作を制御する制御部11と、サーバ装置6A、6Bが接続されるインターフェースポートA、B毎に、入10出力を制御するインターフェースコントローラ12(12A、12B)と、インターフェースポートA、B毎に入出力されるデータを一時的に記憶するFIFO13(13A、13B)と、キャッシュメモリ14を制御するキャッシュコントローラ15と、ハードディスク3が接続されるアクセスポートa～d毎に入出力されるデータを一時的に記憶するFIFO16(1156a～16d)と、各アクセスポートa～dに接続されているハードディスク3(3a～3d)を制御するデバイスコントローラ17と、を備えている。インターフェースコントローラ12は、SCSIやIDE等のインターフェースによりサーバ装置6A、6Bとの接続を制御する。デバイスコントローラ17は、アクセスポートa～dに接続されているハードディスク203に対するデータの読み出しや、書き込みを制御する。

以下、図11に示したネットワークシステムを適用したカルテシステムを例にして本願発明の実施形態の動作を説明する。

ハードディスク3には、テキストファイル形式で患者毎にカルテが記憶されている。各患者には、識別番号が付与されている。ハードディスク253に記憶されているカルテは、該当患者の識別番号(この発明で言う素性コード)と、この患者についてのカルテのシリアル番号(この発明で言う個数コード)と、を含むファイル名で管理されている。ハードディスク3

に記憶されているカルテのファイルネームは、

患者の識別番号ーシリアル番号. t x t

である（図13参照）。患者の識別番号とシリアル番号とは「-」で区切られている。このため、患者の識別番号をキーにすれば、ハードディスク3に記憶されている所望の患者のカルテを検索することができる。また、ハードディスク3に所望の患者のカルテが複数記憶されている場合、シリアル番号により最新のカルテを検索することができる。この実施形態では、ファイルネームに含まれているシリアル番号が大きい程、新しいカルテである。

10 まず、図14を参照しながら医師が端末装置5を操作して、ハードディスク3に記憶されている患者のカルテを読み出すときの、アクセス制御装置1の動作について説明する。

医師は、端末装置5を操作し、該端末装置5をサーバ装置6Aに接続する。医師は、端末装置5がサーバ装置6Aに接続されると、ハードディスク3に記憶されている、カルテの読み出要求をサーバ装置6Aに送信する。サーバ装置6Aは、端末装置5から送信されてきた要求をアクセス制御装置1のインターフェースポートAに転送する。

なお、この実施形態ではサーバ装置6Aは、ネットワーク4を介して端末装置5からハードディスク3に対するアクセスの要求があったとき、このアクセスの要求の種類（カルテの読み出、新規書込、書換、削除）に関係なく、該要求をアクセス制御装置1に転送する。

インターフェースコントローラ12Aは、インターフェースポートAにハードディスク3に対するアクセスの要求が入力されると（s60）、該要求がカルテの読み出要求であるかどうかを判定する（s61）。インターフェースコントローラ12Aは、s61でカルテの読み出要求でないと判定すると（カルテの新規書込、書換、または削除にかかる要求であれば）、今回のハードディスク3に対するアクセスの要求を無視して本処理を終了する

。

このように、アクセス制御装置1は、インターフェースポートAに入力されたハードディスク3に対するアクセスの要求がカルテの読出要求以外の要求であれば、該要求を無視する。

5 なお、ハードディスク3に対するアクセスの要求がカルテの読出要求であるかどうかをサーバ装置6Aに判定させ、サーバ装置6Aがカルテの読出要求以外の要求であると判定したときに、該要求をインターフェースポートAに転送しないように構成してもよい。

10 インタフェースコントローラ12Aは、s21でカルテの読出要求であると判定すると、今回インターフェースポートAに入力されたカルテの読出要求をキャッシュコントローラ15を介してデバイスコントローラ17に転送する(s62)。s22でデバイスコントローラ17に転送されるカルテの読出要求には、カルテを読み出す患者の識別番号が含まれている

。

15 デバイスコントローラ17は、s62で転送してきたカルテの読出要求に含まれている識別番号をキーにしてアクセスポートa～dに接続されているハードディスク3a～3dを検索し(s63)、該当する患者のカルテを読み出す(s64)。このとき、デバイスコントローラ17は、読出要求に含まれている識別番号を用いて、ハードディスク3に記憶されている該当する患者のカルテを検索し、さらに、ここで検索したカルテの中でファイルネームに含まれているシリアル番号が最も大きいカルテ、すなわち識別番号で識別される患者についての最新のカルテ、を読み出す。

20 s64でハードディスク3a～3dから読み出されたカルテは、キャッシュメモリ14に書き込まれる。デバイスコントローラ17は、s63におけるカルテの読出を完了すると(s65)、その旨をキャッシュコントローラ15に通知する(s66)。

25 キャッシュコントローラ15は、デバイスコントローラ17からカル

テの読み完了が通知されると、インターフェースコントローラ 12A に対して、カルテの読み完了を転送する (s 67)。また、キャッシングコントローラ 15 は、キャッシングメモリ 14 に記憶した該当するカルテをインターフェースコントローラ 12A に転送する (s 68)。キャッシングコントローラ 15 は、s 68 においてキャッシングメモリ 14 に記憶されている該当するカルテを順次読み出し FIFO 13A に記録する。

キャッシングコントローラ 15 からカルテの読み完了が転送されてきたインターフェースコントローラ 12A は、FIFO 13A に記憶されているカルテを順番に読み出し、インターフェースポート A に接続されているサーバ装置 6A へ出力する (s 69)。

サーバ装置 6A は、アクセス制御装置 1 から送信されてきたカルテを、今回カルテの読み要求を送信してきた端末装置 5 にネットワーク 4 を介して送信する。

したがって、ユーザは、端末装置 5 において、ネットワーク 4 介して接続したサーバ装置 6A に、ハードディスク 3a～3d に記憶されているカルテの読み要求を送信することにより、該読み要求に含めた識別番号で識別される患者の最新のカルテを得ることができる。このため、医師は端末装置 5 で任意の患者の最新のカルテを簡単に確認することができる。

次に、図 15 を参照しながら、医療行為が終了した患者のカルテをハードディスク 3a～3d に新規に書き込むときのアクセス制御装置 1 の動作について説明する。医師は、患者に対する今回の医療行為が完了すると、端末装置 5 において先に読み出した患者のカルテに今回の医療行為の内容を追加する。上述のように、カルテはテキストファイルであるので、簡単な操作で今回の医療行為の内容をカルテに追加できる。医師は、今回の医療行為の内容を追加したカルテを作成すると、端末装置 5 をサーバ装置 6B に接続し、ハードディスク 3 に対するカルテの書き要求を送信する。この書き要求には、今回の医療行為の内容が追加されたカルテおよび患者

の識別番号が含まれている。

サーバ装置 6 B は、端末装置 5 から送信されてきた要求をアクセス制御装置 1 のインターフェースポート B に転送する。

なお、この実施形態ではサーバ装置 6 B は、ネットワーク 4 を介して  
5 端末装置 5 からハードディスク 3 に対するアクセスの要求があったとき、  
このアクセスの要求の種類（データの読出、新規書込、書換、削除）に関  
係なく、該要求をアクセス制御装置 1 に転送する。

インターフェースコントローラ 12 B は、インターフェースポート B にハ  
ードディスク 3 に対するアクセスの要求が入力されると（s 7 0）、該要  
10 求がカルテの新規書込要求であるかどうかを判定する（s 7 1）。インターフェースコントローラ 12 B は、s 7 1 でカルテの新規書込要求でないと  
判定すると（カルテの読出、書換、または削除にかかる要求であれば）、  
今回のハードディスク 3 に対するアクセスの要求を無視して本処理を終了  
する。

15 このように、アクセス制御装置 1 は、インターフェースポート B に入力  
されたハードディスク 3 に対するアクセスの要求がカルテの新規書込要求  
以外の要求であれば、該要求を無視する。

なお、ハードディスク 3 に対するアクセスの要求がカルテの書込要求  
であるかどうかをサーバ装置 6 B に判定させ、該サーバ装置 6 B が新規書  
20 込要求以外の要求であると判定したときに、該要求をインターフェースポート B に転送しないように構成してもよい。

インターフェースコントローラ 12 B は、s 3 1 でカルテの新規書込要求  
であると判定すると、今回インターフェースポート B に入力されたカルテ  
の新規書込要求をキャッシュコントローラ 15 を介してデバイスコントロ  
25 ラ 17 に転送する（s 7 2）。このとき、インターフェースコントローラ  
12 B は、インターフェースポート B に入力された今回の医療行為の内容が  
追加されたカルテを F I F O 13 B に順次書き込んで行く。キャッシュコ

ントローラ 15 は、FIFO 13B に書き込まれたカルテを順次読出、キャッシュメモリ 14 に確保した空き領域に書き込む。

キャッシュコントローラ 15 からカルテの新規書込要求が転送されてきたデバイスコントローラ 17 は、該新規書込要求に含まれている患者の 5 識別番号をキーにしてハードディスク 3a～3d を検索し、今回ハードディスク 3a～3d に記憶するカルテのファイルネームを決定する (s 73)。具体的には、書込要求に含まれている識別番号を含むファイルネームでハードディスク 3a～3d に記憶されているカルテを検索し、さらに、ここで検索したカルテの中でファイルネームに含まれているシリアル番号 10 の最大値を判断する。デバイスコントローラ 17 は、今回記憶するカルテのファイルネームのシリアル番号を、ここで判断した最大値を 1 カウントアップした値に決定する。

なお、ファイルネームに含まれる識別番号は、書込要求に含まれている患者の識別番号である。

15 デバイスコントローラ 17 は、s 73 でハードディスク 3a～3d に書き込むカルテのファイルネームを決定すると、ハードディスク 3a～3d の空き領域に今回の医療行為の内容が追加されたカルテを書き込む (s 74)。このとき、デバイスコントローラ 17 は、キャッシュメモリ 14 に書き込まれた該当するカルテを順次読出、該カルテを記憶させるハード 20 ディスク 3a～3d が接続されているアクセスポート a～d に接続されている FIFO 16 に書き込む。ハードディスク 3 は、FIFO 16 から順次読み出したカルテをハードディスク 3a～3d の空き領域に記憶する。

25 このように、端末装置 5 において、ハードディスク 3a～3d への患者のカルテの新規書込が行える。すなわち、最初に患者のカルテを読み出して、このカルテに新たな医療行為の内容が追加されたものを新規書込する。この実施形態では、ハードディスク 3a～3d にカルテを新規に書き込むとき、ハードディスク 3a～3d に記憶されている該当患者のカルテ

を削除したり、記憶している該当患者のカルテに上書き（書換）しないので、医師による端末装置 5 の誤操作が生じても、ハードディスク 3 a～3 d にすでに記憶されているカルテが破壊されることはない。また、ハードディスク 3 a～3 d に記憶されたカルテは、削除したり書き換えることが 5 できないので、悪意を持った者の不正なアクセスにより、ハードディスク 3 a～3 d に記憶されているカルテが改竄されたり、削除されたりするのも防止できる。

また、アクセス制御装置 1 は、カルテの読出時には患者の識別番号をキーにしてハードディスク 3 a～3 d に記憶されているカルテの中から該 10 当患者の最新のカルテを読み出すことができ、またカルテの書込時には患者の識別番号を用いてハードディスク 3 a～3 d に書き込むカルテのファイルネームを自動的に決定するので、端末装置 5 における医師の操作性を低下させることもない。

また、端末装置 5 を操作する医師は、これから行う操作を意識して接 15 続するサーバ装置 6 A または 6 B を選択しているので（ハードディスク 3 a～3 d に記憶されているカルテを読み出すときにはサーバ装置 6 A に接続し、ハードディスク 3 a～3 d にカルテを書き込むときにはサーバ装置 6 B に接続する。）、医師による誤操作の発生頻度も抑えられる。但し、医師による誤操作が発生しても、上述のようにハードディスク 3 a～3 d 20 に記憶されているカルテの書き換えや、削除については防止できる。ハードディスク 3 a～3 d に記憶されているカルテを十分に保護できる。また、医師のカルテへのアクセスは、通常、カルテを読み出して、医療行為の内容を追加して書き込む、ということなので、端末 5 において、カルテへのアクセス操作（例えばカルテボタンの操作）を行えば、自動的にサーバ装置 6 A に接続されて読み出し状態となり、次に、もう一度カルテボタン 25 の操作が行われると、自動的にサーバ装置 6 B に接続されて書き込み状態となるようにプログラムすることも可能である。

また、患者毎にカルテの更新履歴として、ハードディスク 3 a～3 d に記憶させてカルテが全て残っているので、カルテの改竄が行われても、改竄の有無を判断することができる。

また、上記実施形態ではインターフェースポート A はカルテの読出のみ許可され、インターフェースポート B はカルテの新規書込のみ許可されるとしたが、インターフェースポート A、B 共に、カルテの読出、および新規書込の両方を許可し、読出、書込以外の要求（書換、削除等）を無視するように構成してもよい。この場合、アクセス制御装置 1 は、インターフェースポート A、B にハードディスク 3 に対するアクセスの要求が入力されると 10 、該アクセスの要求がカルテの読出であるか、カルテの新規書込であるか、カルテの読出、新規書込以外であるかを判断し、カルテの読出であれば上記 s 6 2 以降の処理を行い、カルテの新規書込であれば上記 s 7 2 以降の処理を行い、カルテの読出、新規書込以外であれば無視するように構成すればよい。

15 なお、上記実施形態では、ハードディスク 3 a～3 d にカルテをテキストファイル形式で記憶させるとしたが、印刷イメージの形式で記憶させてもよいし、他のファイル形式で記憶させてもよい。また、本願発明は上記カルテシステム以外のネットワークシステムにも適用できる。

また、上記実施形態では、カルテの書込み時にカルテ全体を書き換えるとしたが、医師が今回追加した内容（医師による今回の診療内容）を該当患者のカルテに追加記録（アpend）するようにしてもよい。このよう 20 にすれば、患者のカルテを記憶するのに必要なハードディスク 3 a～3 d の記憶容量を抑えることができる。

また、上記実施形態では、ハードディスク 3 a～3 d に記憶されているカルテについては、書換、削除ができないとしたが、管理者等にパスワードを与える、削除が行えるようにしてもよい。このようにすれば、ハードディスク 3 a～3 d に記憶されている不要なカルテ取り除くことができ、

患者のカルテを記憶するのに必要なハードディスク 3 a～3 d の記憶容量を抑えることができる。但し、この場合も書換については行えないようにしておくのが好ましい。

以上のように、この発明によれば、ユーザの誤操作、故意の操作、不正アクセスによって、該記憶装置に記憶されているデータが改竄、破壊、削除されるのを防止することができる。これにより、記憶装置に記憶されているデータのセキュリティを向上させることができる。

### 産業上の利用分野

10 本発明は、患者の病歴や医療行為等が記録されているカルテに対する不法改竄行為や、LAN、インターネットに接続されているサーバへのハッキング、クラッキングによる不法書き込み行為等を防ぐ装置に適用することができる。

## 請 求 の 範 囲

(1) 外部機器が接続される複数のインターフェースポートと、  
5 データを記憶する記憶装置が接続されるアクセスポートと、  
上記インターフェースポート毎に、上記記憶装置に対して許可するア  
クセスの種類を設定し、上記記憶装置に対するアクセスの要求がいずれかの  
インターフェースポートに入力されたとき、該インターフェースポートに対し  
て許可されているアクセスの種類に基づいて、入力されたアクセスの要求  
10 の実行可否を判断する制御部と、を備えたアクセス制御装置。

(2) 上記アクセスポートを複数備え、  
上記制御部は、異なるアクセスポートに接続されている複数の記憶裝  
置にデータを分割して記憶させる請求項1に記載のアクセス制御装置。

(3) 上記アクセスポートを複数備え、  
15 上記制御部は、異なるアクセスポートに接続されている複数の記憶裝  
置に同じデータを記憶させる請求項1に記載のアクセス制御装置。

(4) 請求項1に記載のアクセス制御装置と、  
上記アクセスポートに接続された記憶装置と、を有するデータ管理裝  
置。

20 (5) 外部機器が接続されるインターフェースポートと、  
データを記憶する記憶装置が接続される複数のアクセスポートと、  
上記アクセスポート毎に、接続されている上記記憶装置に対して許可  
するアクセスの種類を設定し、いずれかのアクセスポートに接続されてい  
る上記記憶装置に対するアクセスの要求が上記インターフェースポートに入  
25 力されたとき、アクセスが要求された上記記憶装置が接続されている上記  
アクセスポートに対して許可されているアクセスの種類に基づいて、入力  
されたアクセスの要求の実行可否を判断する制御部と、を備えたアクセス

制御装置。

(6) 外部機器が接続される複数のインターフェースポートと、  
データを記憶する記憶装置が接続される複数のアクセスポートと、  
上記インターフェースポート毎に、各記憶装置に対して許可するアクセ  
5 スの種類をそれぞれ設定し、上記記憶装置に対するアクセスの要求がいず  
れかのインターフェースポートに入力されたとき、該インターフェースポート  
から該アクセスポートに対して許可されているアクセスの種類に基づいて  
、入力されたアクセスの要求の実行可否を判断する制御部と、を備えたア  
クセス制御装置。

10 (7) 外部機器が接続されるインターフェースポートと、  
記憶装置が接続されるアクセスポートと、  
上記アクセスポートに接続された上記記憶装置に対して許可するアクセ  
セスの種類をデータの読出および新規書込に設定し、上記インターフェース  
ポートに入力された上記記憶装置に対するアクセスの要求が、データの読  
15 出または新規書込のいずれかであれば入力されたアクセスの要求を実行し  
、データファイルの読出または新規書込以外の要求であれば入力されたア  
クセスの要求を無視する制御部と、を備えたアクセス制御装置。

(8) 外部機器が接続される複数のインターフェースポートと、  
記憶装置が接続されるアクセスポートと、  
20 上記インターフェースポート毎に、上記アクセスポートに接続された上  
記記憶装置に対して許可するアクセスの種類をデータの読出または新規書  
込の一方に設定し、データの読出を許可した上記インターフェースポートに  
入力された上記記憶装置に対するアクセスの要求が、データの読出であれば  
25 入力されたアクセスの要求を実行し、データの読出以外の要求であれば  
入力されたアクセスの要求を無視し、さらにデータの新規書込を許可した  
上記インターフェースポートに入力された上記記憶装置に対するアクセスの  
要求が、データの新規書込であれば入力されたアクセスの要求を実行し、

データの新規書込以外の要求であれば入力されたアクセスの要求を無視する制御部と、を備えたアクセス制御装置。

(9) 上記制御部は、上記記憶装置に新規書込したデータに対して、該データの素性を示す素性コードと、その時点で該素性コードが同じデータの個数を示す個数コードと、を含むファイルネームを付与する請求項1に記載のアクセス制御装置。

(10) 請求項1に記載のアクセス制御装置と、  
該アクセス制御装置の上記アクセスポートに接続された記憶装置と、  
を有するデータ記憶装置。

(11) 医師が操作する端末機器からのカルテデータの読み出要求、又は新規書込要求が入力される複数のインターフェースポートと、  
カルテデータが記憶されている記憶装置が接続されるアクセスポートと、

上記インターフェースポート毎に、上記アクセスポートに接続された上記記憶装置に対して許可するアクセスの種類をデータの読み出または新規書込の一方に設定し、データの読み出を許可した上記インターフェースポートに入力された上記記憶装置に対するアクセスの要求が、データの読み出であれば入力されたアクセスの要求を実行し、データの読み出以外の要求であれば入力されたアクセスの要求を無視し、さらにデータの新規書込を許可した上記インターフェースポートに入力された上記記憶装置に対するアクセスの要求が、データの新規書込であれば入力されたアクセスの要求を実行し、データの新規書込以外の要求であれば入力されたアクセスの要求を無視する制御部と、を備えたアクセス制御装置。

1/15

図1

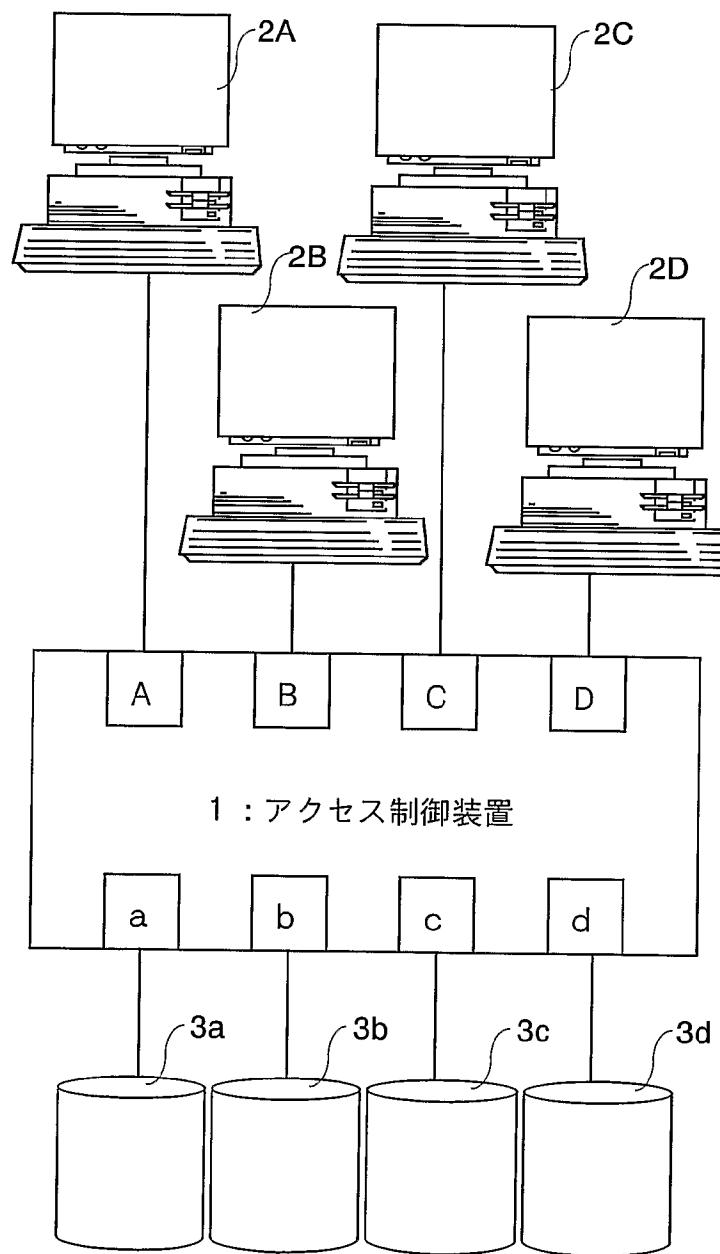


図2

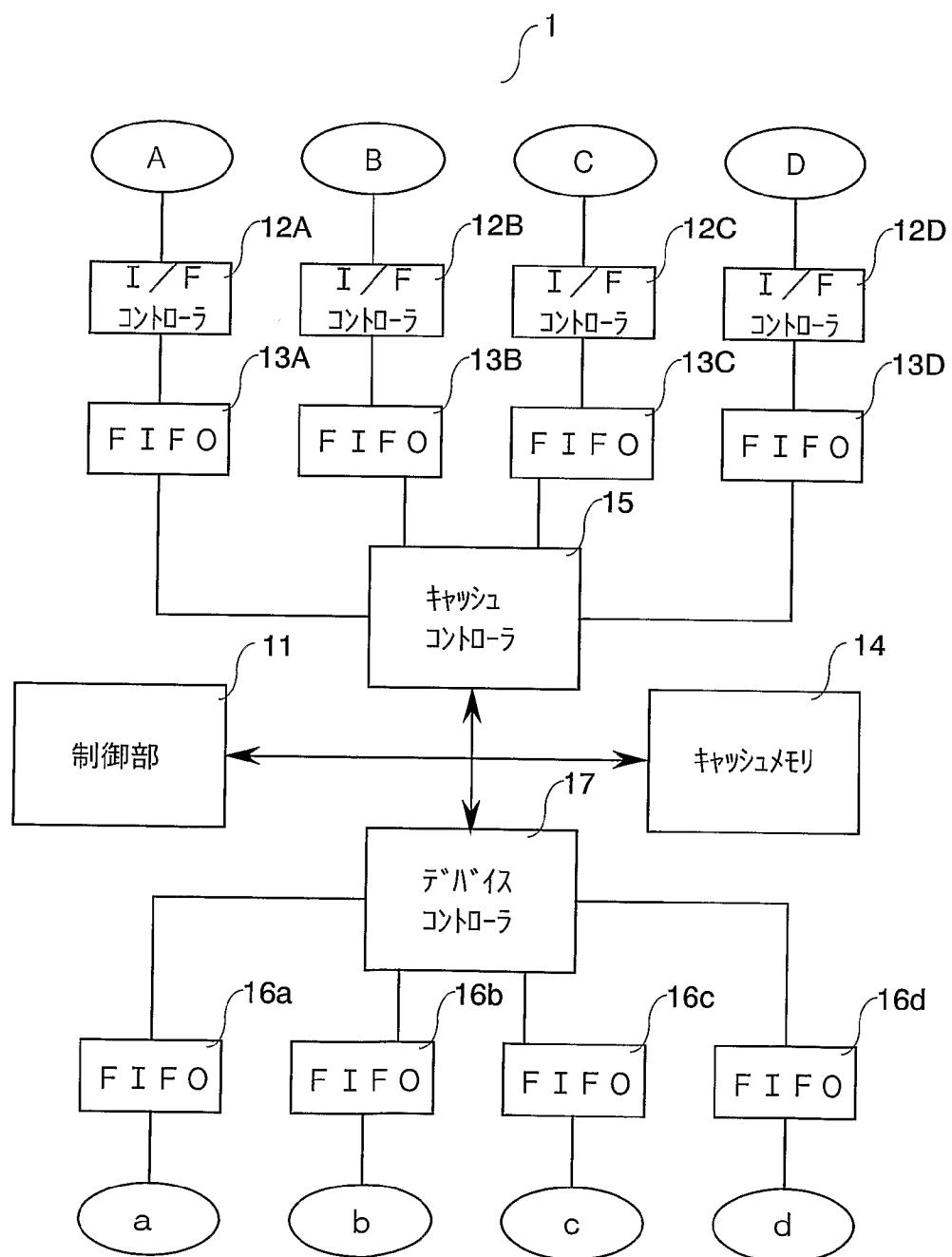


図3

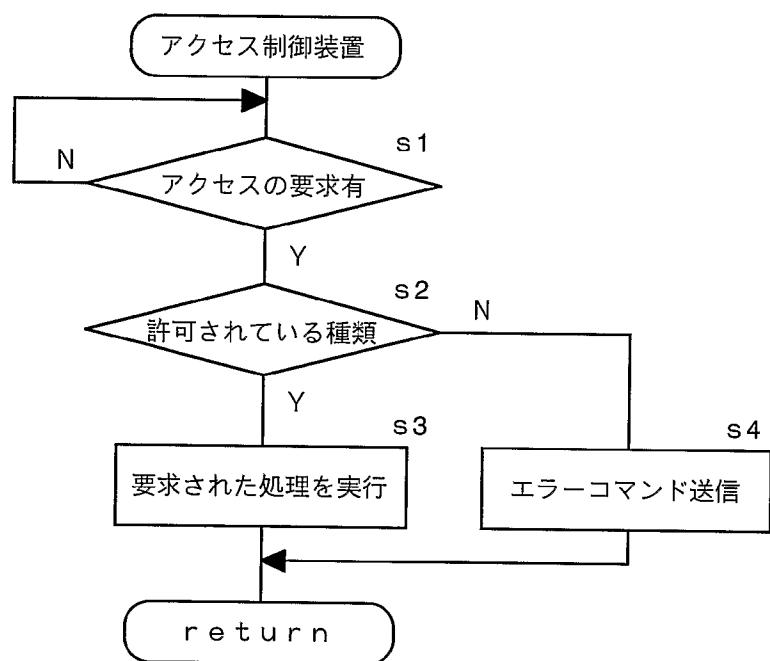


図4

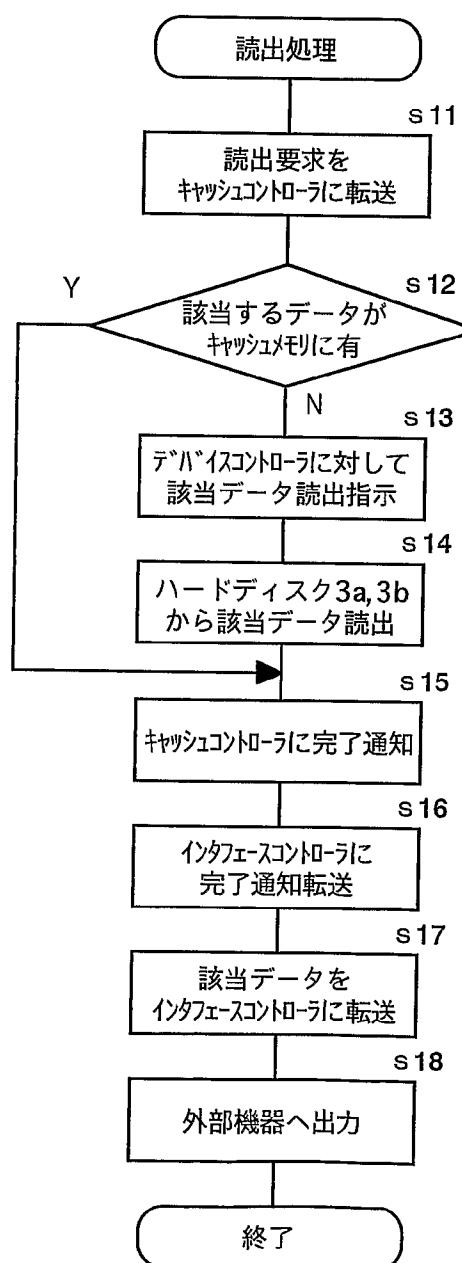
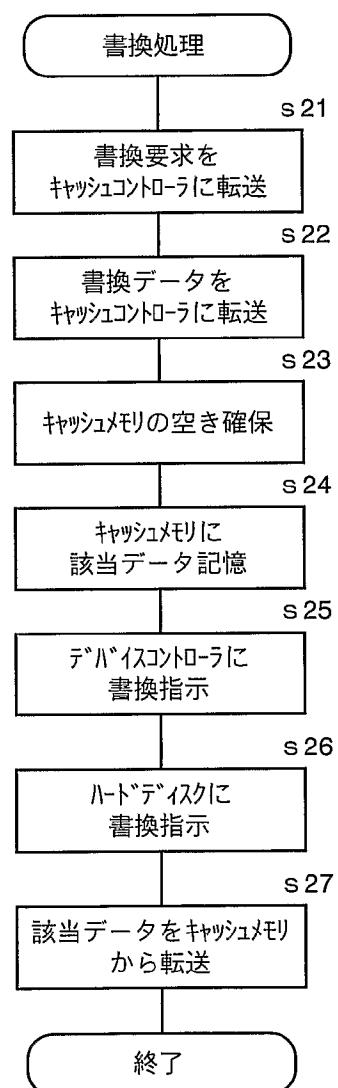
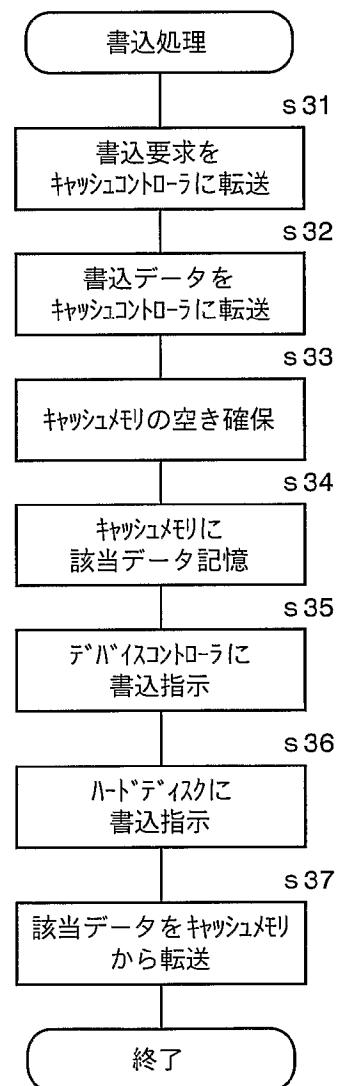


図5



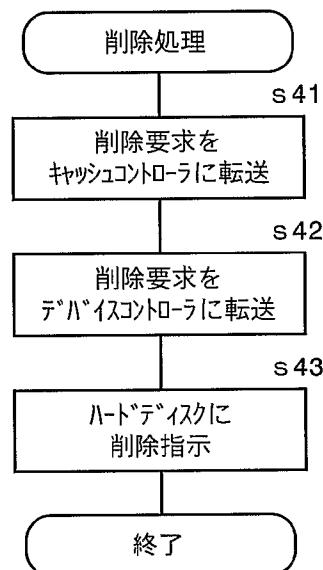
6/15

図6



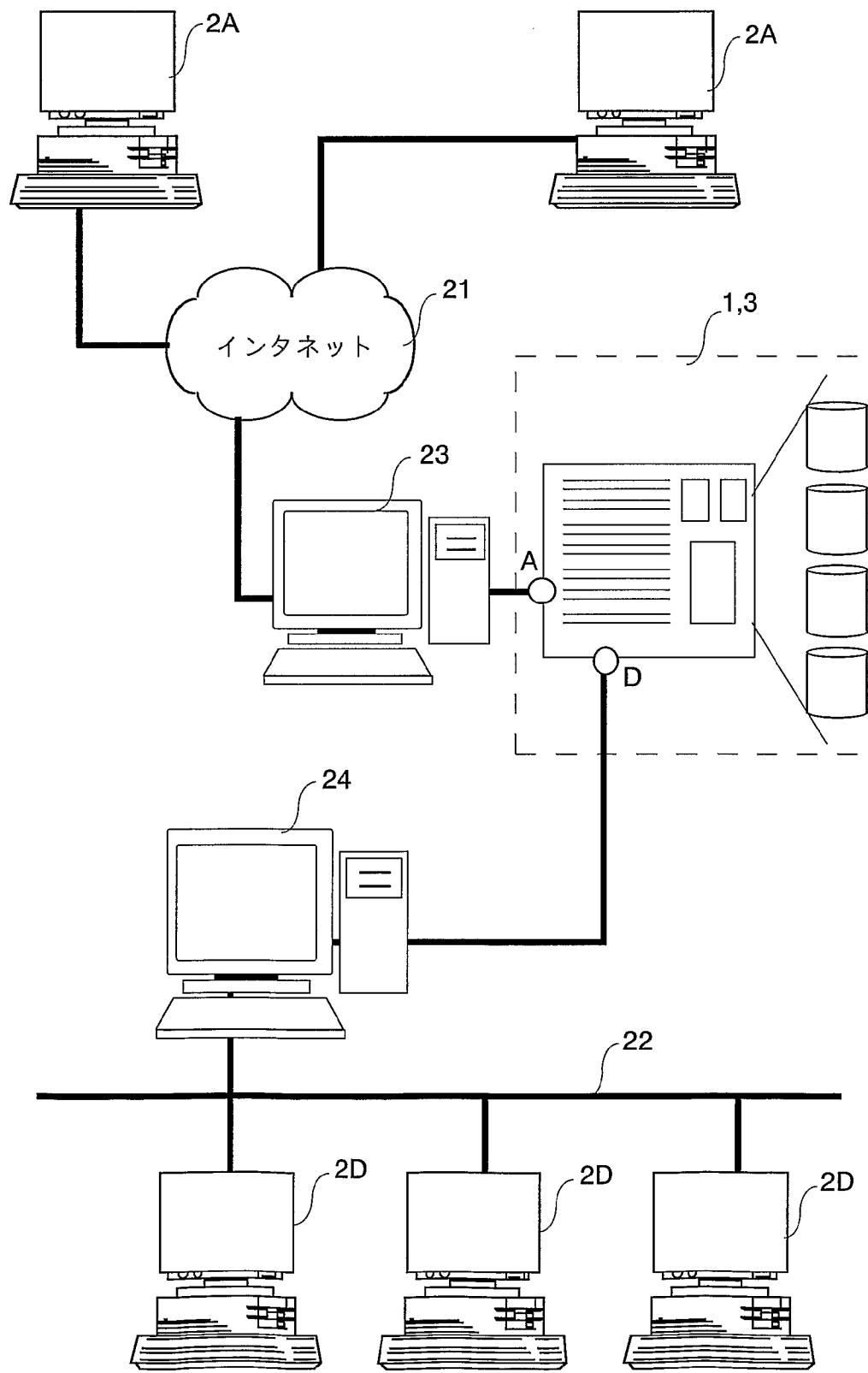
7/15

図7



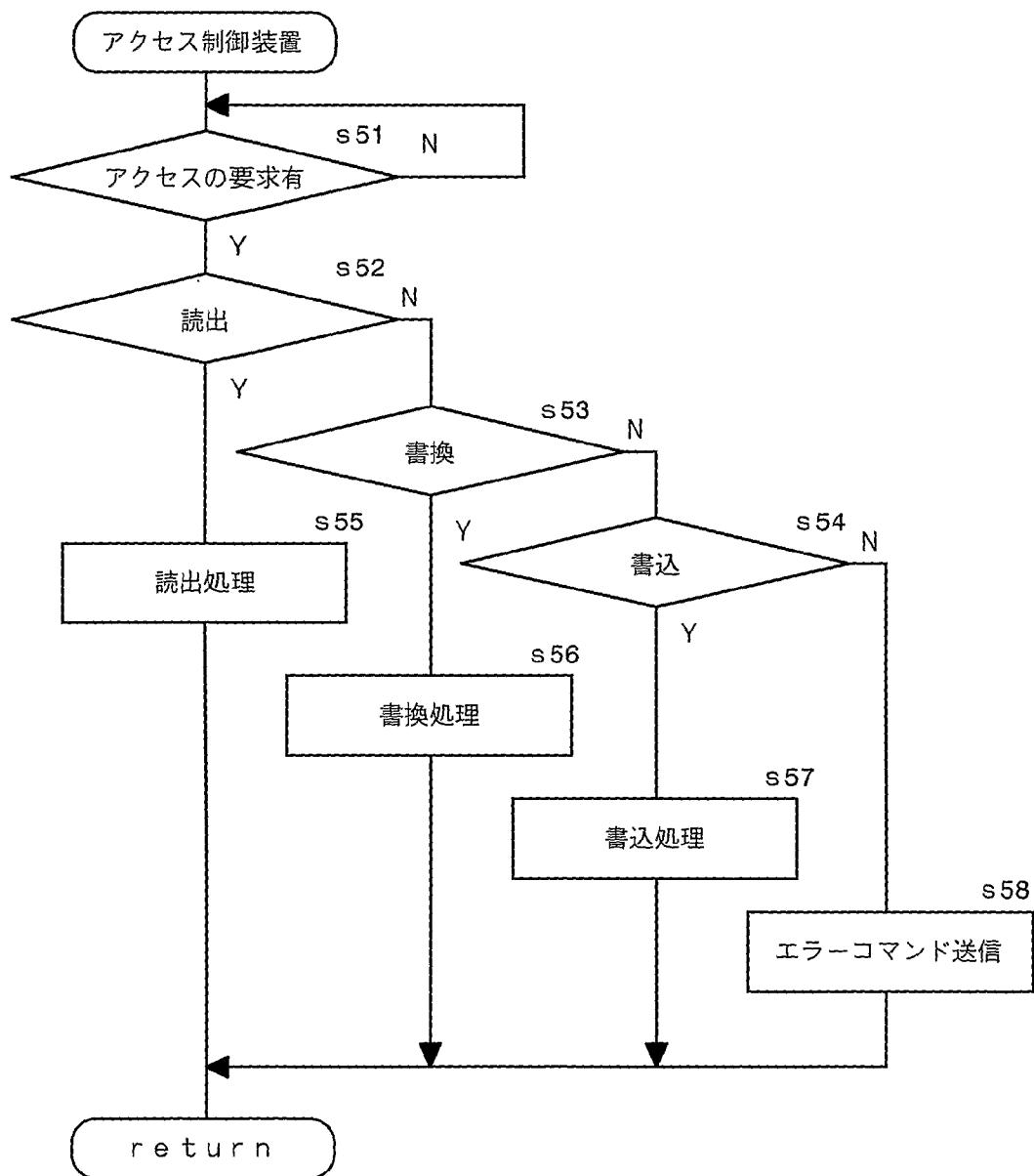
8/15

図8



9/15

図9



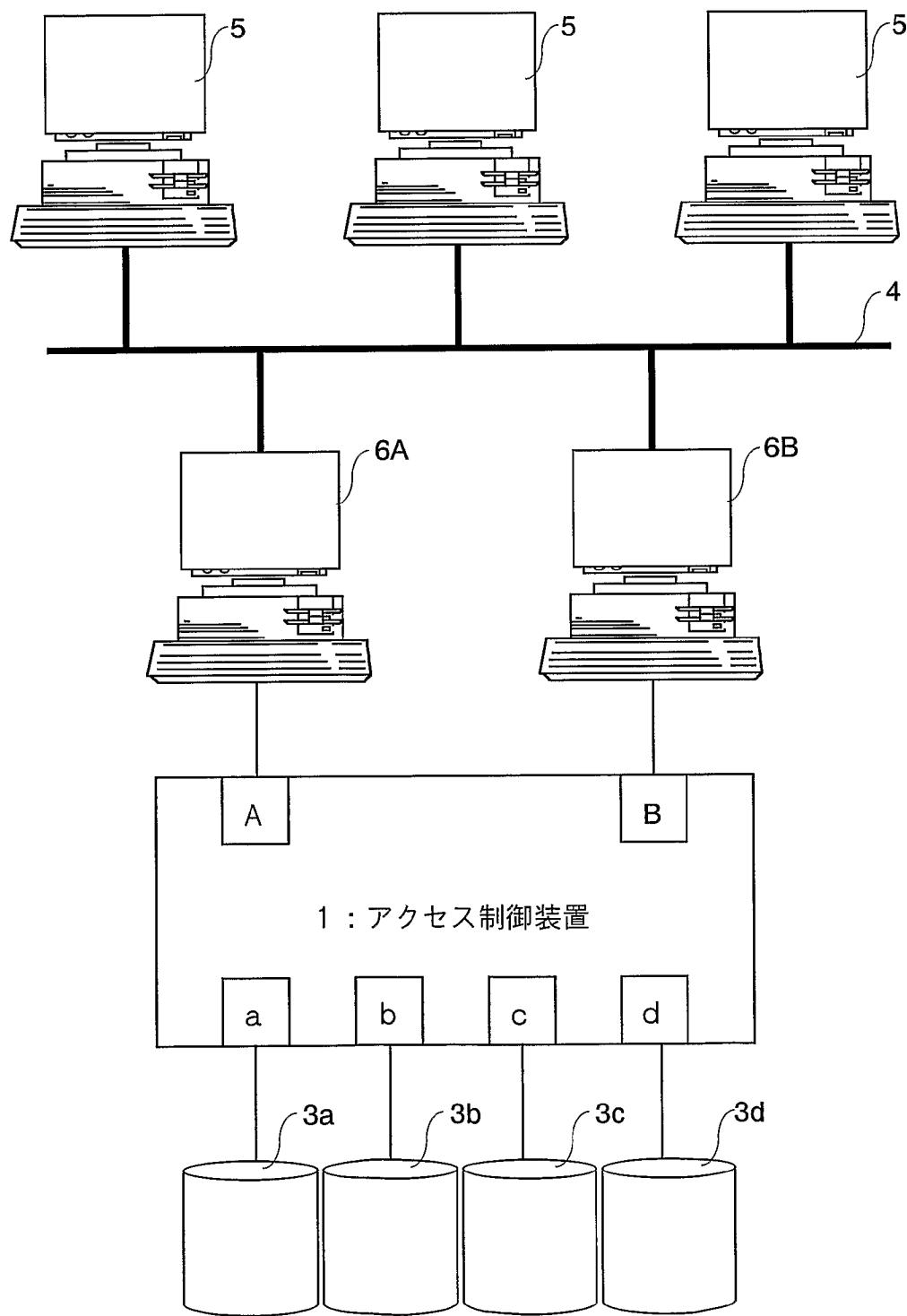
10/15

図10

	I/Fport-A	I/Fport-B	I/Fport-C	I/Fport-D
アクセス port-A	読出	読出	書換	書込
アクセス port-B	×	書換	書込 書換	読出
アクセス port-C	×	書込	読出	書換
アクセス port-D	×	×	×	×

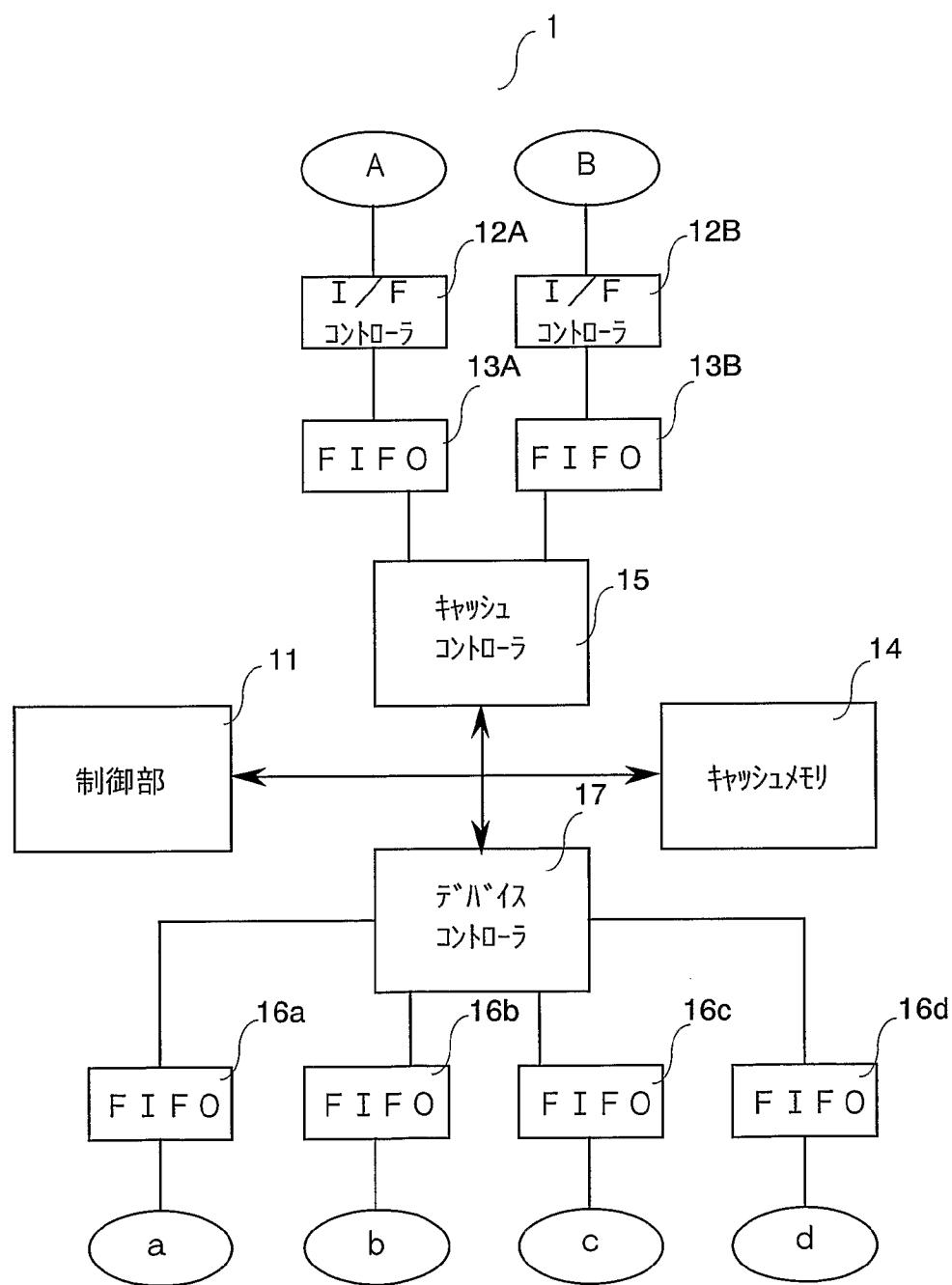
11/15

図11



12/15

図12



13/15

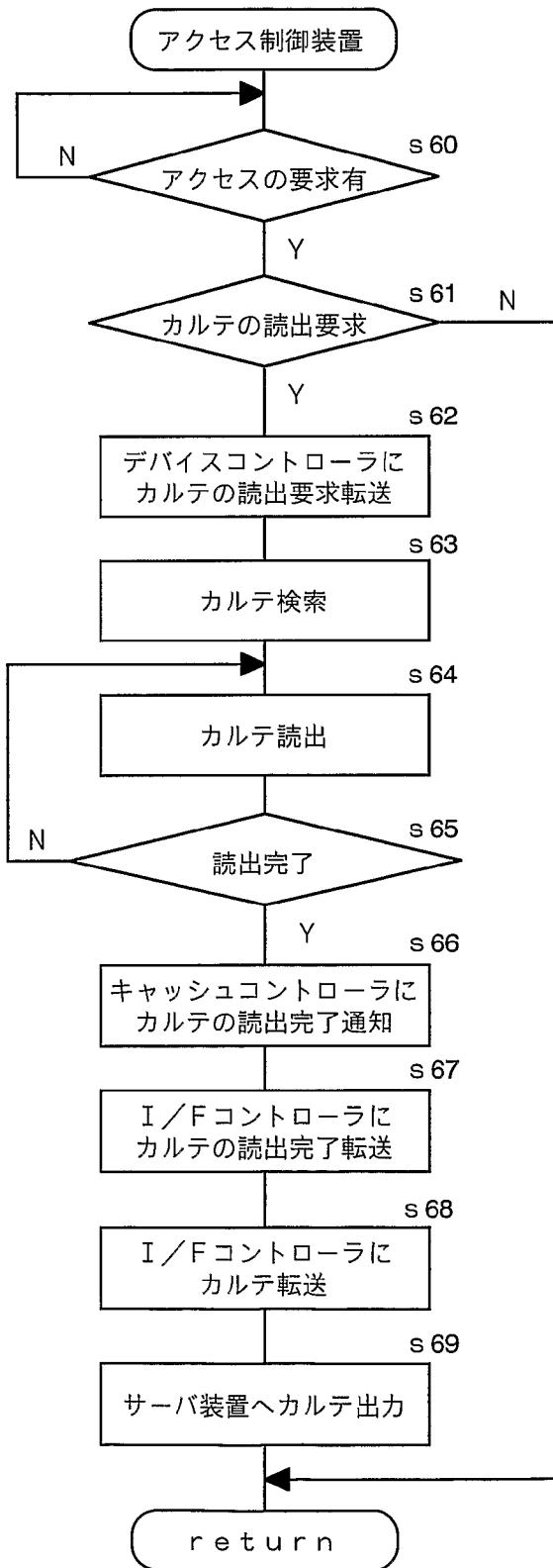
図13

識別番号 シリアル番号

1 2 3 4 5 6 7 8 - 0 0 5 . t x t

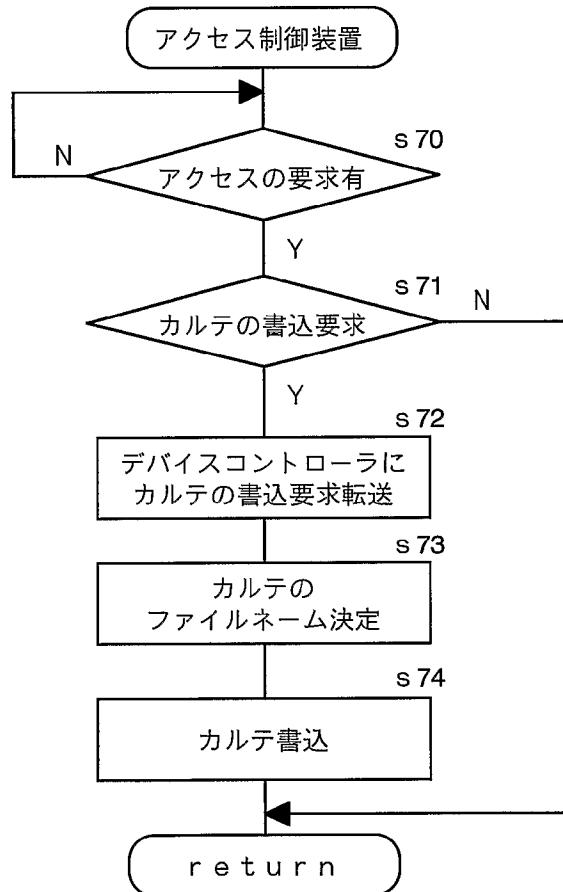
14/15

図14



15/15

図15



# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/03701

## A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl<sup>7</sup> G06F13/14, G06F12/14, G06F3/06

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl<sup>7</sup> G06F13/14, G06F12/14, G06F3/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2003
Kokai Jitsuyo Shinan Koho	1971-2003	Jitsuyo Shinan Toroku Koho	1996-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

JICST FILE [AKUSESUSEIGYO and KARUTE]

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 4-333973 A (Hitachi, Ltd.), 20 November, 1992 (20.11.92), Column 1, lines 1 to 12; Figs. 2, 6 (Family: none)	1-11
Y	JP 10-275106 A (Telecommunications Advancement Organization of Japan, Hitachi, Ltd., Hitachi Engineering & Services Co., Ltd.), 13 October, 1998 (13.10.98), Full text; Fig. 1 (Family: none)	1, 4-11
Y	JP 10-105346 A (Hitachi, Ltd.), 24 April, 1998 (24.04.98), Column 2, lines 32 to 34, 46 to column 3, line 1 (Family: none)	2-3

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search

01 July, 2003 (01.07.03)

Date of mailing of the international search report

15 July, 2003 (15.07.03)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP03/03701

**C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2002-032251 A (Hitachi, Ltd.), 31 January, 2002 (31.01.02), Full text (Family: none)	3
A	JP 2001-034690 A (Sanyo Electric Co., Ltd.), 09 February, 2001 (09.02.01), Full text (Family: none)	1, 4-11

## A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. C17 G06F 13/14, G06F 12/14, G06F 3/06

## B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. C17 G06F 13/14, G06F 12/14, G06F 3/06

## 最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年  
 日本国公開実用新案公報 1971-2003年  
 日本国登録実用新案公報 1994-2003年  
 日本国実用新案登録公報 1996-2003年

## 国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

JICST科学技術文献ファイル [アクセス制御 and カルテ]

## C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 4-333973 A (株式会社日立製作所) 1992.11.20, 第1欄, 第1-12行, 第2, 6図 (ファミリーなし)	1-11
Y	JP 10-275106 A (通信・放送機構, 株式会社日立製作所, 株式会社日立エンジニアリングサービス) 1998.10.13, 全文, 第1図 (ファミリーなし)	1, 4-11
Y	JP 10-105346 A (株式会社日立製作所) 1998.04.24, 第2欄, 第32-34行, 第2欄, 第46	2-3

 C欄の続きにも文献が列挙されている。 パテントファミリーに関する別紙を参照。

## \* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの  
 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの  
 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)  
 「O」口頭による開示、使用、展示等に言及する文献  
 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

## の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの  
 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの  
 「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの  
 「&」同一パテントファミリー文献

国際調査を完了した日 01.07.03	国際調査報告の発送日 15.07.03
国際調査機関の名称及びあて先 日本国特許庁 (ISA/JP) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官 (権限のある職員) 石井 茂和 電話番号 03-3581-1101 内線 6790

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	行—第3欄、第1行 (ファミリーなし) JP 2002-032251 A (株式会社日立製作所) 2002. 01. 31, 全文 (ファミリーなし)	3
A	JP 2001-034690 A (三洋電機株式会社) 2001. 02. 09, 全文 (ファミリーなし)	1, 4-11